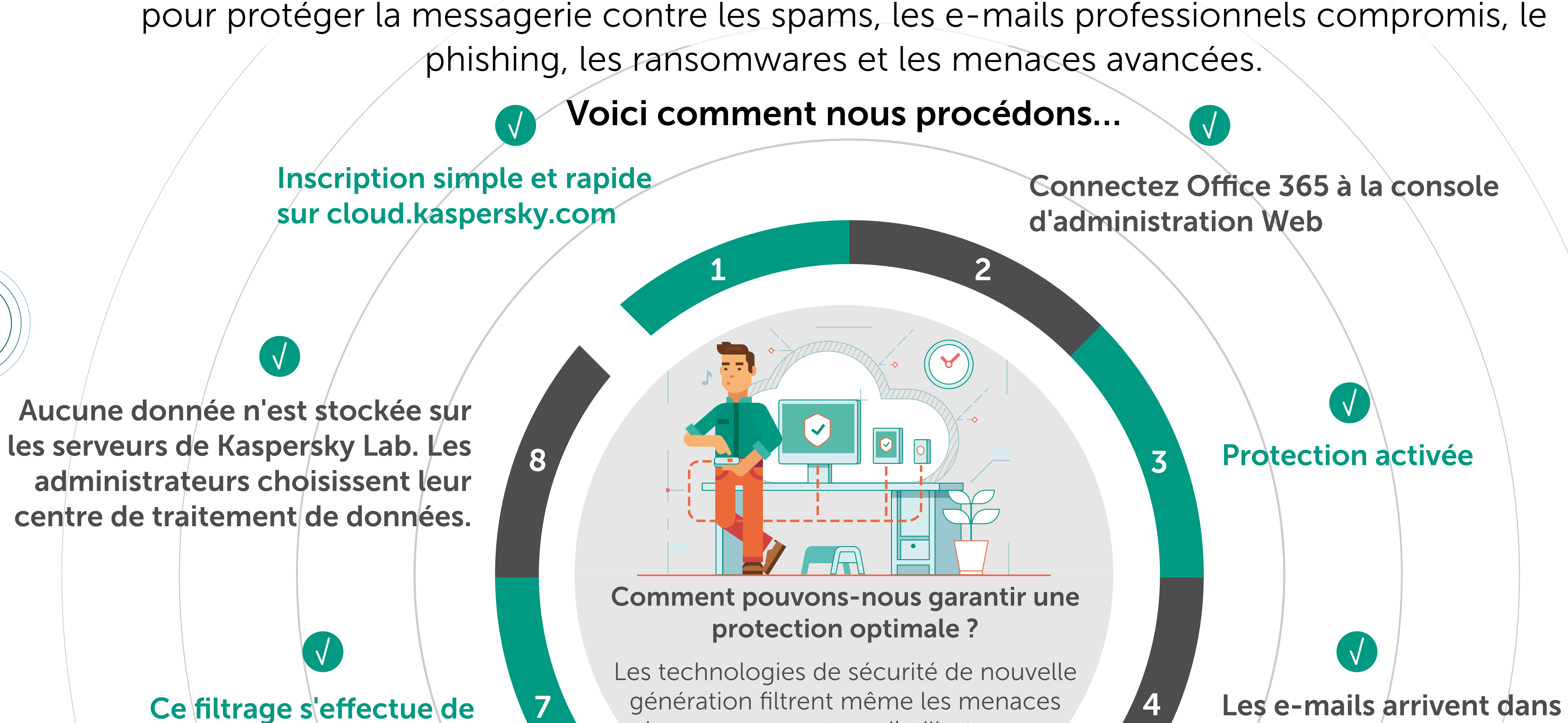
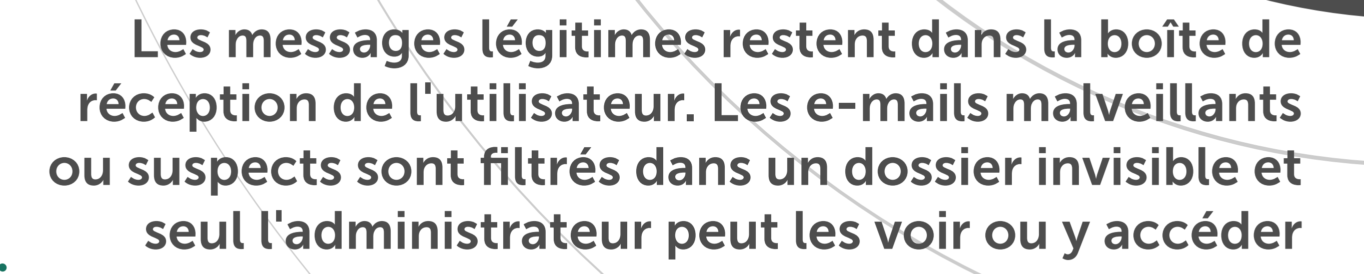
Comment fonctionne
Kaspersky Security for Microsoft Office 365

Kaspersky Security for Microsoft Office 365 utilise des technologies de nouvelle génération pour protéger la messagerie contre les spams, les e-mails professionnels compromis, le phishing, les ransomwares et les menaces avancées.

Voici comment nous procédons...



1. **Inscription simple et rapide sur cloud.kaspersky.com**
2. **Connectez Office 365 à la console d'administration Web**
3. **Protection activée**
4. **Les e-mails arrivent dans votre Cloud Office 365**
5. **Kaspersky Security for Microsoft Office 365 les analyse pour détecter les menaces**
6. **Les messages légitimes restent dans la boîte de réception de l'utilisateur. Les e-mails malveillants ou suspects sont filtrés dans un dossier invisible et seul l'administrateur peut les voir ou y accéder**
7. **Ce filtrage s'effectue de manière rapide et efficace**
8. **Aucune donnée n'est stockée sur les serveurs de Kaspersky Lab. Les administrateurs choisissent leur centre de traitement de données.**



Comment pouvons-nous garantir une protection optimale ?

Les technologies de sécurité de nouvelle génération filtrent même les menaces inconnues avant que l'utilisateur ne puisse commettre une erreur.

Technologie anti-spam de nouvelle génération

Les modèles de détection issus du Machine Learning de Kaspersky Lab détectent les courriers indésirables inconnus, même sophistiqués, tout en réduisant le nombre de faux positifs.

Détection multi-niveau grâce à la surveillance HuMachine

Identifie même les programmes malveillants inconnus. Les fichiers suspects peuvent être exécutés dans un espace de sécurité avant d'en autoriser la réception.



Machine Learning

Les algorithmes de Machine Learning sont entraînés pour identifier les programmes malveillants sur des ensembles composés de plus de **200 millions** de fichiers malveillants et **1 milliard** de fichiers sains. Ces modèles de détection filtrent les programmes malveillants « zero-hour » jusque-là inconnus.



Big Data / Threat Intelligence

Threat Intelligence mondiale sur les menaces basée dans le Cloud et mise à jour en continu, assurée par Kaspersky Security Network. Combinée à l'expertise humaine de plus de 200 experts.



Filtrage des pièces jointes :

Le filtrage des pièces jointes bloque les fichiers dangereux avant qu'ils ne deviennent un problème. La reconnaissance de type de fichier filtre aussi bien les contenus indésirables que malveillants.



Antiphishing de nouvelle génération

Le moteur antiphishing basé sur les réseaux de neurones artificiels de Kaspersky Lab utilise plus de 1 000 critères pour établir les modèles de détection.